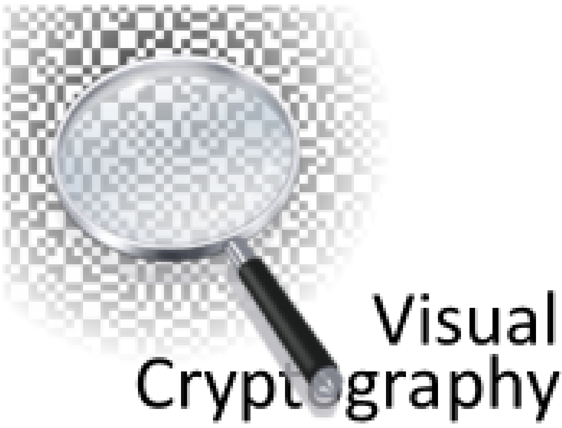
Dhirubhai Ambani
Institute of Information and Communication Technology

SC402: INTRODUCTION TO CRYPTOGRAPHY

-Prof. Manish Gupta

Visual Cryptography and implementation

Group 10:
201901011 - Himanshu Dudhatra
201901024 - Dhavalsinh Raj
201901100 - Shubham Patel
201901143 - Akshat Patel



Introduction

Nowadays, almost everything is happening on the internet, and every kind of transition and data transfer is done online. Because of the internet's architecture and operation, it is possible for anyone to intentionally or unintentionally misuse data. If the data is secret, this can cause significant problems for the individual, organization, or government. In most circumstances, mathematical methods are employed to transform the format of the data into other formats in such a way that it is incomprehensible to the observer if the data is obtained, and these types of techniques are known as cryptography. So for security purposes, cryptography methods are handy to encrypt and decrypt data. If confidential data is like images, text, diagrams, etc., then visual cryptography is used for security purpose.

Visual cryptography was developed by Moni Naor and Adi Shamir. Visual cryptography varies from other cryptographic approaches in that it focuses on human eyesight to decrypt secret information rather than complicated mathematical equations or decryption hardware. It is quite desirable to be able to conceal information such as personal details. When data is concealed within different images, it becomes absolutely unidentifiable. In this process main secret image is split into two separate noisy images that are totally different in look compared to the original image and to get the original image back (decryption) we need to superimpose two separate images. Naor and Shamir extended this fundamental idea to a k out of n secret sharing problem ((k, n) scheme), where n is the total number of shares and k is the smallest number of shares required to recover the secret.

Visual Cryptography

Visual cryptography is a cryptographic approach that allows us to encrypt visual data such as images, text, diagrams, and so on in such a way that the decrypted data is almost identical to the original visual image. The image is split into n shares for encryption in this method. If someone receives n-1 shares, no information about the original image is revealed. The image can only be decrypted by the person who owns all of the shares. By overlaying all n shares, the original image can be decrypted.

How Visual Cryptography works

Visual Cryptography can be used to perform one-time pad encryption. The image is split into two component images in this technique: a random pad and a cipher text. Take a binary image first as a secret image. A binary image has either black or white pixels. Each pixel in a secret image is now divided into four(2x2) small subpixels as given in the below Figure 1.

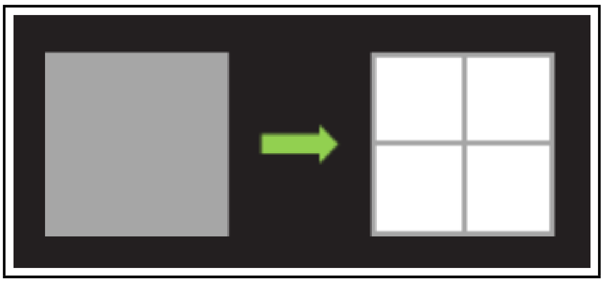


Figure 1. Divide pixels into 4 subpixels (reference)

The original secret image's pixels are colored black or white by using the following rules: If the secret image's pixel is black, the component image's pixel pairs should be complementary, and if the secret image's pixel is white, the component image's pixel pairs should be similar and you can see this in below Figure 2.

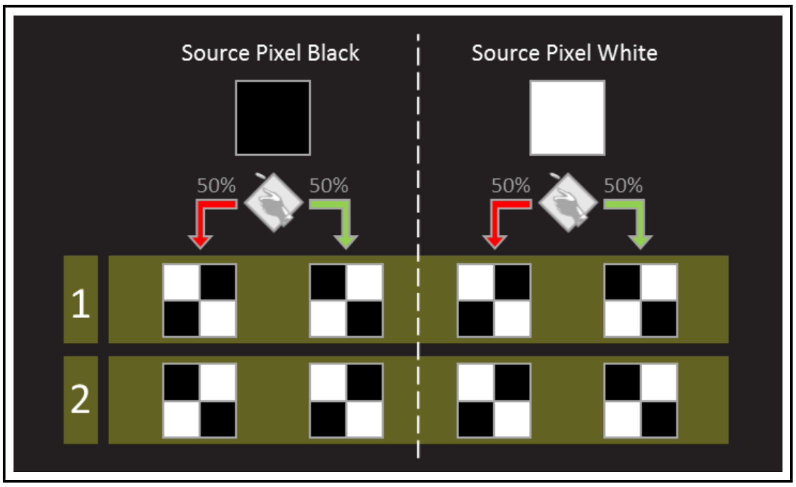


Figure 2. Black pixel and White pixel (reference)

We can get the original secret image by merging the two component images, which means decryption. Only one component image can't reveal any information, as we all know. You must have both component images for decryption.

The decrypted image will be four times as large as the original so the contrast of the decrypted image will be half of the original secret image. The black pixels of the original secret image will remain black in the decrypted image, but the white pixels will be changed into half-tone grey color. But this contrast is sufficient enough to read the secret image. The snapshot of Visual Cryptography working of our implementation code is given below in Figure 3. First, the SECRET IMAGE is turned into binary image by performing Black and White image generation. Then SECRET IMAGE BW is split(encryption) into two shares: SHARE 1 and SHARE 2 by using above mentioned pixel algorithm. After overlaying both shares(decryption), the stacked result appears like RESULT IMAGE which is quite similar to the secret image.

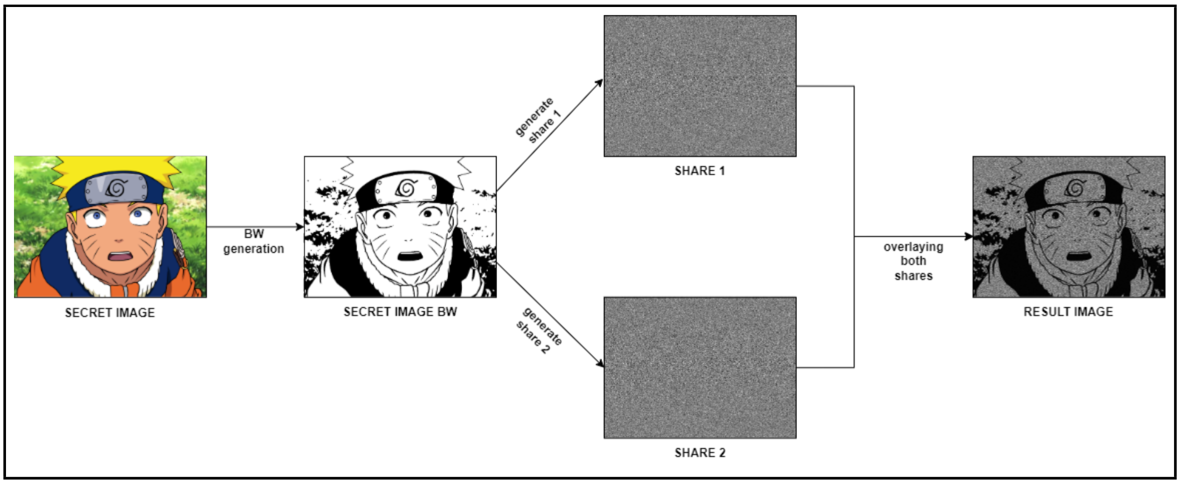


Figure 3. Visual Cryptography

Visual Steganography

We can perform something more interesting with Visual Cryptography. Let's say we have two source images and a third secret image that we want to encrypt. The technique for hiding secret images within other simpler images is called as Visual Steganography. We want to create two cipher images that appear to be simple but hide a third hidden image. Transparencies can be used to print the two cipher pictures. They are designed to replicate simple images. The third secret image appears when these two cipher images are merged. See Figure 4 below.

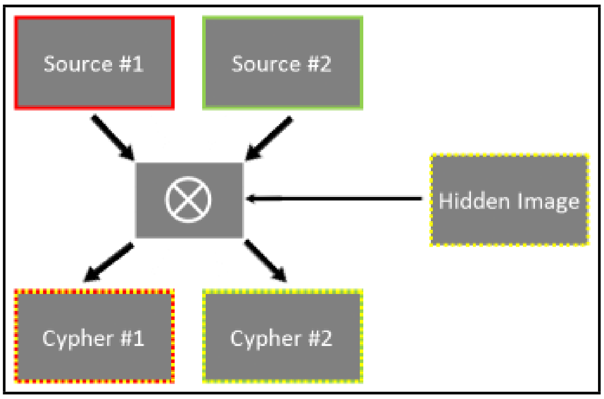


Figure 4. Visual Steganography (reference)

How Visual Steganography works

The secret image in visual steganography contains both black and white pixels. As previously, we split each pixel into four (2x2) subpixels. We represent the hidden image's black pixels when all four subpixels are black, and the white pixels when any three subpixels are black when the two images are combined. This provides sufficient contrast to reveal the hidden image. For each black or white pixel of the hidden image, there are four different combinations of source image subpixels. The black pixel is represented by any three black subpixels in both source pictures, while the white pixel is represented by any two black subpixels. All permutations of source images 1 and 2 are given below in Figure 5.

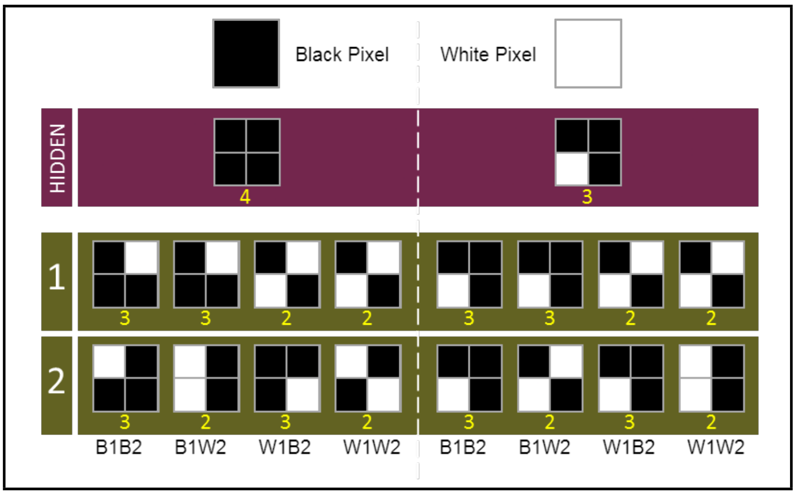


Figure 5. Black and White pixel (reference)

- When the pixel is black in the hidden image:

  1. The combined cipher images must have all four subpixel sets.
  2. When both images have black pixels, the condition is that both source images must have three black subpixels and the missing subpixel must not same. One subpixel is selected randomly from the first black layer, and one is selected randomly from the other three subpixels from the second black layer.
  3. When one image has a black pixel (three black subpixels) and another image has a white pixel (two black subpixels), one subpixel is selected randomly from the first black layer to remove, and the next two subpixels are selected randomly from the second white layer such that one of the selected subpixels can fill the gap of the first layer. We get four black subpixels when the two are combined.
  4. The opposite happens when the first layer is white and the second layer is black.
  5. When both pixels are white (two black subpixels), two subpixels are selected randomly from the first white layer and the mirror selection is selected from the second white layer.

- When the pixel is white in the hidden image:

  1. The combined cipher images must have all four subpixel sets.
  2. When both images have black pixels, the condition is that both source images must have three black subpixels same. Three subpixels are selected randomly for both layers.
  3. When one image has a black pixel (three black subpixels) and another image has a white pixel (two black subpixels), three subpixels are selected randomly from the first black layer, and the next one of those three subpixels is selected randomly to remove and this pattern with two black subpixels is used for the second white layer.
  4. The opposite happens when the first layer is white and the second layer is black.
  5. When both pixels are white (two black subpixels), two subpixels are selected randomly from the first white layer, one of them is similar to the second white layer, and the second subpixel is selected randomly on the second layer with the condition of selecting from the two white subpixels of the first white layer.

The snapshot of Visual Steganography working of our implementation code is given below in Figure 6. First, the two SOURCE IMAGEs are turned into binary image by performing Black and White image generation. The binary image of the HIDDEN IMAGE is also generated by performing Black and White image generation. Considering both SOURCE IMAGE BWs and HIDDEN IMAGE BW, generate two CIPHER IMAGES that looks like two SOURCE IMAGES by using above mentioned pixel algorithm. At decryption, by overlaying both CIPHER IMAGEs, original hidden image is appears as RESULT IMAGE which looks like the HIDDEN IMAGE.

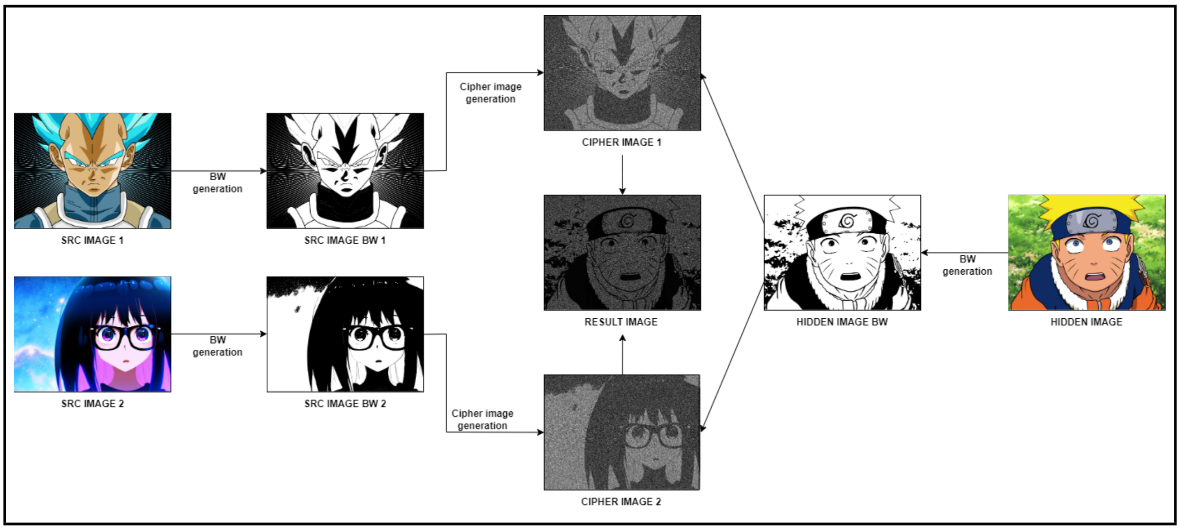


Figure 6. Visual Steganography

Implementation code

Visual Cryptography and Visual Steganography implementation code: GitHub link

References

[1] Visual Cryptography and Visual Steganography

[2] A Comprehensive Study of Visual Cryptography

[3] Visual Cryptography

[4] An Overview of Visual Cryptography Techniques

[5] Schemes and Applications of Visual Cryptography